

### **REMARKS**

Applicants appreciate the thorough examination of the present application as shown in the Office Action of February 8, 2006 (hereinafter "Office Action"). In response, Applicants have amended the pending claims to clarify the distinctions between the recitations thereof and the cited references. In particular, independent Claim 1 has been amended to remove the recitation of "receiving a reset code as the authorization code and over-riding the usage specification responsive to receipt of the reset code". Independent Claims 22 and 30, which respectively recite systems and computer program products corresponding to the method of Claim 1, have been similarly amended. Also, Claim 32 has been amended to depend from Claim 22, as requested by the Examiner.

Accordingly, Applicants respectfully submit that the pending claims are patentable over the cited references for at least the reasons discussed below.

#### **The Claim Objections**

Claim 32 has been objected to based on informalities, and in particular, for incorrectly reciting dependency from Claim 1. *See* Office Action, Page 2. In response, Applicants have amended Claim 32 to depend from Claim 22, as requested by the Examiner. Accordingly, Applicants respectfully request withdrawal of the objection to Claim 32.

#### **The Section 103 Rejections**

Claims 1, 2, 9-13, 15, 16, 18, 19 and 22-24 have been rejected under 35 USC §103(a) as being obvious over U.S. Patent No. 5,884,193 to Kaplan (hereinafter "Kaplan") in view of U.S. Patent No. 5,517,554 to Mitchell et al. (hereinafter "Mitchell"). Office Action, Page 3. In addition, Claims 3-8, 20 and 25-29 have been rejected under 35 USC §103(a) as being obvious over Kaplan in view of Mitchell and U.S. Patent Application Publication No. 2004/0203601 to Morriss et al. (hereinafter "Morriss"). Office Action, Page 9. Also, Claims 14, 17, 21, 31, and 32 have been rejected under 35 USC §103(a) as being obvious over Kaplan in view of Mitchell and U.S. Patent Application Publication No. 2004/0209595 to Bikanich (hereinafter "Bikanich"). Office Action, Page 12. Claim 1 as amended, for example, recites:

1. A method for controlling usage of a mobile terminal, the method comprising:

receiving a usage specification including an identification of allowed numbers, an identification of restricted numbers, a usage time limitation, an expiration value and/or a specification of enabled services of the mobile terminal that are restricted; and

limiting usage of the mobile terminal based on the received usage specification responsive to receipt of a valid authorization code; and

wherein receiving a usage specification and limiting usage further comprise at least one of the following:

receiving a usage specification restricting access to enabled services of the mobile terminal including internet access services, multimedia messaging access services, email services, camera and/or video functions; and/or

receiving the authorization code wherein the authorization code is encoded to restrict viewing of the authorization code by a user of the mobile terminal. (*Emphasis added*).

The Office Action asserts that the combination of Kaplan and Mitchell discloses the recitations of Claim 1 as amended. *See* Office Action, Page 3. For example, the Office Action concedes that Kaplan fails to disclose at least the portions of Claim highlighted above, but asserts that Mitchell teaches at least one of the highlighted recitations of Claim 1. More particularly, the Office Action asserts that Mitchell discloses an authorization code that is encoded to restrict viewing of the authorization code by a user of the mobile terminal. *See* Office Action, Page 4.

Mitchell is directed to an apparatus and method for locking a mobile identification number (MIN) of a mobile communication unit at a mobile switching center, to thereby prevent use of the mobile communication unit. *See* Mitchell, Abstract. For example, as described in Mitchell:

When the user purchases the mobile communication unit, the mobile communication unit is assigned a mobile identification number (MIN) and electronic serial number (ESN) which are used to identify the mobile communication unit when it operates within the cellular communication system, and therefore, identifies the user for billing purposes. When in use, the mobile communication units communicate, via radio transmission, with base station transceivers within the cellular communication system. The base station transceivers further communicate with a base station controller which in turn communicates with a mobile switching center (MSC). From the MSC, a user can be connected to other cellular communication system users or to public switch telephone network (PSTN) users. In establishing communications within the cellular system, the mobile communication unit is required to broadcast, over the air, the MIN and the ESN. This is required so that the mobile switching center serving the cellular communication system can identify the mobile communication unit operating in the cellular

communication system so that calls placed or received by the mobile communication unit may be properly identified and billed.

Mitchell, Col. 1, lines 14-35 (*emphasis added*). In other words, the MIN is broadcast from the mobile terminal for purposes of identification of the mobile terminal and/or associated communications in a cellular system.

In its assertion that Mitchell discloses the authorization code of Claim 1, the Office Action cites Column 1, lines 57-59 of Mitchell. *See* Office Action, Page 4. However, as provided in the paragraph corresponding to cited portion of Mitchell:

As a result of such cellular communication system fraud, cellular system operators are subject to extensive losses of revenue. In response, methods to combat the fraudulent use of mobile identification numbers have been developed. For example, it is known to scramble or otherwise encrypt the MIN and ESN during broadcast. This makes intercepting a MIN substantially more difficult. The MIN may still be intercepted, however, and once a MIN is intercepted, it can be used to fraudulently access the cellular communication system.

Mitchell, Col. 1, lines 53-62 (*emphasis added*). As such, the Office Action appears to assert that the scrambled and/or encrypted MIN described in the portion of Mitchell cited above corresponds to an authorization code that "is encoded to restrict viewing by a user of the mobile terminal", as recited in Claim 1.

Applicants respectfully disagree. As discussed in the portion of Mitchell cited above, the scrambling and/or encrypting of the MIN appears to be concerned with interception of the MIN *during broadcast*. More particularly, as further described in Mitchell:

Cellular pirates, fraudulent users of the cellular communication system, have developed methods of intercepting the MIN and ESN numbers during such broadcasts when the mobile communication unit is operating in the cellular communication system. The cellular pirates have also developed methods of programming "clone" mobile communication units with the intercepted MIN and ESN numbers. When a clone mobile communication unit accesses the system, the cellular system recognizes the MIN and ESN as being valid and allows the call to proceed. The call, however, is billed to the legitimate cellular user whose mobile communication unit was programmed with the intercepted MIN and ESN. Ultimately, the cellular system operator absorbs losses due to fraudulent calls by not collecting for the fraudulent calls and from lack of system use by legitimate users who have lost confidence in the system.

Mitchell, Col. 1, lines 36-52 (*emphasis added*). As such, the MIN does not appear to be encoded to restrict viewing thereof *by a user of the mobile terminal*, but rather by "*cellular pirates*" who may intercept the MIN during broadcast and use the MIN to fraudulently access the cellular communication system.

Moreover, nowhere do the cited portions of Mitchell appear to disclose or suggest that the MIN is an "authorization code" as recited by Claim 1. Rather the MIN is used for identification of the mobile terminal by the cellular system, as discussed above. Thus, Applicants respectfully submit that Mitchell does not disclose or suggest receiving an authorization code "wherein the authorization code is encoded to restrict viewing of the authorization code by a user of the mobile terminal", as recited in Claim 1.

The Office Action further asserts that it would be obvious to modify the invention of Kaplan based on the encrypted MIN of Mitchell "for the purpose of securing the device". See Office Action, Page 4. However, Applicants respectfully submit that, to establish a *prima facie* case of obviousness, the prior art reference or references when combined must teach or suggest *all* the recitations of the claims, and there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. See MPEP § 2143. The mere fact that references can be combined or modified does not render the resultant combination obvious unless the prior art also suggests the desirability of the combination. See MPEP § 2143.01(citing *In re Mills*, 916 F.2d 680, 16 U.S.P.Q.2d 1430 (Fed. Cir. 1990)). In addition, as emphasized by the Court of Appeals for the Federal Circuit, to support combining references, evidence of a suggestion, teaching, or motivation to combine must be *clear and particular*, and this requirement for clear and particular evidence is not met by broad and conclusory statements about the teachings of references. *In re Dembiczak*, 50 U.S.P.Q.2d 1614, 1617 (Fed. Cir. 1999).

Applicants respectfully submit that one of skill in the art would not be motivated to combine the teachings of Mitchell with those of Kaplan, and that the references themselves provide no such suggestion or motivation. More particularly, as discussed above, Mitchell is directed to preventing use of a mobile communication unit by locking the mobile identification number (MIN) of the mobile communication unit at the mobile switching center (MSC). For example, Mitchell provides:

The present invention provides an apparatus and method for locking a mobile communication unit by locking the mobile identification number (MIN) assigned to the mobile communication unit at the mobile switching center (MSC). Once a MIN is locked at the MSC, access will be denied to any mobile communication unit attempting to originate a call in the cellular communication system with the locked MIN, even if it is the mobile communication unit legitimately assigned the locked MIN which is attempting to place the call.

Mitchell, Col. 2, lines 42-51 (*emphasis added*). In other words, Mitchell describes controlling usage of a mobile terminal *at the mobile switching center*. Furthermore, Mitchell describes operations for controlling the *general* ability of the mobile terminal to place and/or receive calls based on identification of the mobile terminal by its MIN.

In contrast, Kaplan is directed to systems and methods for call restriction in a wireless communication device. See Kaplan, Abstract. More particularly, as described in Kaplan:

The present invention is embodied in a system **100**, illustrated in the functional block diagram of FIG. 1. The system 100 can be readily implemented by any wireless communication device, such as a cellular telephone, personal communication system (PCS) device, wireless local loop (WLL) telephone, or the like. However, for the sake of clarity, the following paragraphs describe an implementation of the system 100 within a cellular telephone. The system 100 advantageously processes call restrictions within the wireless communication device itself rather than rely on call restriction processing at a cell site controller (not shown).

Kaplan, Col. 3, lines 35-45 (*emphasis added*). In other words, Kaplan describes restricting usage of a mobile terminal *within the mobile terminal itself*. In addition, Kaplan provides that "[t]he system uses a pre-designated calling plan and includes an enable signal having enabled and disabled states to selectively enable call origination from the wireless communication device". Kaplan, Col. 1, lines 59-62 (*emphasis added*). Examples of the specific call restrictions discussed in Kaplan include restrictions on local, long-distance, and/or international calling. See Kaplan, Col. 7, lines 44-64.

Accordingly, Applicants submit that one of skill in the art would not be motivated to combine operations performed *at a mobile switching center* for preventing *general* use of a mobile terminal (as described in Mitchell) with operations performed *at the mobile terminal* for restricting *specific* uses of the mobile terminal (as described in Kaplan). Moreover, Applicants

submit that the Office Action's broadly stated motivation "for the purpose of securing the device" is not "clear and particular", as required by the case law cited above.

Furthermore, even if the teachings of Kaplan and Mitchell were combined, Applicants submit that the combination would not disclose or suggest the recitations of Claim 1 as amended. For example, the operations for encrypting a broadcast MIN to prevent interception thereof described in Mitchell would not appear to be of help in restricting the viewing of an authorization code in the device of Kaplan, as Kaplan does not employ an authorization code that is broadcast and/or otherwise transmitted and the operations of Kaplan are performed within the mobile terminal itself. Moreover, the complete restriction of use of the mobile terminal described in Mitchell appears to teach away from the stated advantages described in Kaplan, in particular, that "[t]he present invention advantageously provides various levels of call restriction that can be selected by the user and implemented within the wireless communication device itself." Kaplan, Col. 3, lines 31-33 (*emphasis added*).

Accordingly, Applicants submit that Kaplan and Mitchell fail to disclose or suggest at least the recitations of Claim 1 as amended highlighted above, and that it would not be obvious to combine the teachings of Kaplan and Mitchell for at least the reasons discussed above.

Applicants note that Claim 1 also recites "a usage specification restricting access to enabled services of the mobile terminal including internet access services", and that, in rejecting Claim 14, the Office Action relies on Beganich as disclosing similar recitations. *See* Office Action, Page 13. As such, Applicants will address some of the arguments presented in the Office Action with regard to the teachings of Beganich with reference to the recitations of Claim 1. More particularly, Applicants submit that Beganich does not disclose or suggest "a usage specification restricting access to enabled services of the mobile terminal including internet access services". For example, as described in the cited portions of Beganich:

**FIG. 14D** illustrates an exemplary monitoring process performed when an Internet event is detected, as illustrated in step **S40**. An Internet event may be characterized by connecting to one or more of a plurality of servers through website addresses. For example, the mobile station may start counting when the user logs in to an Internet access service. An Internet event may be monitored by the amount of time connected to the Internet and/or counting the number of kilobytes of data sent and received from the Internet, in real time, as illustrated in step S41. The real time counting and timer activity may be displayed during the Internet event, as illustrated in step S42. The monitoring process stops when the end of the data event is detected, such as by detecting

a termination of the Internet session with the service provider network, as illustrated in step S43.

Bekanich, Page 7, Paragraph 0096 (*emphasis added*). In other words, Bekanich describes monitoring the internet access of the mobile terminal, and displaying the amount of time connected and/or the number of kilobytes transferred. More generally, Bekanich is directed to monitoring usage of a wireless communication device associated with particular types of device events, such as Internet events, and providing an alarm to the operator of the device when the usage is close to exceeding a predetermined amount of available usage. *See* Bekanich, Abstract and Page 2, Paragraph [0016]. As such, the cited portions of Bekanich do not disclose or suggest *restricting* usage of the mobile terminal, but rather, *monitoring* usage of the mobile terminal "so as to avoid exceeding the time usage permitted under the basic billing plan and thereby avoid unexpected high monthly bills". Bekanich, Page 1, Paragraph 0007. Thus, Bekanich does not disclose or suggest "receiving a usage specification restricting access to enabled services of the mobile terminal including internet access services, multimedia messaging access services, email services, camera and/or video functions", as recited by Claim 1 as amended. Nor does the Office Action rely on Bekanich as disclosing the other recitations of Claim 1 as amended.

Furthermore, the Office Action does not rely on Morriss to provide the recitations of Claim 1 as amended. Accordingly, Applicants submit that Claim 1 as amended is patentable over the combination of Kaplan, Mitchell, Bekanich, and/or Morriss for at least the above reasons. Claims 22 and 30 recite systems and computer program products corresponding to the method of Claim 1, and as such, are patentable for at least similar reasons. Also, Claims 2-21 and 31, and Claims 23-29 and 32, are patentable at least per the patentability of Claims 1 and 22, from which they, respectively, depend.

In addition, while each of the dependent claims is patentable as depending from Claims 1 or 22, Applicants submit that certain of the dependent claims are also separately patentable over the cited references. For example, Claim 12 recites, in part, "providing a listing of numbers from a phone book of the mobile terminal to a display of the mobile terminal" and "receiving a designation of ones of the displayed listing of numbers". The Office Action asserts that Kaplan discloses these recitations at Col. 8, lines 9-22. *See* Office Action, Page 6. However, as provided by the cited portion of Kaplan:

To set the specific call restriction definitions of **FIG. 4A**, the display may provide the user with guidance in restricting calls such as domestic long distance calls, international long distance calls, and the like using a step-through menu to guide the user in the selection of call restrictions. The call restriction data entered by the user would determine which byte in column **310** corresponds to which restriction definition in column **312**. As previously described, the access to the restriction level storage area **124** would be controlled by a password stored in the password storage area **126**. The different restriction definitions may be referred to by a restriction definition number listed in column **308**. Thus, restriction definition number 1 would correspond to No Domestic Long Distance, and so on.

Kaplan, Col. 8, lines 9-22 (*emphasis added*). As such, although Kaplan generally describes guiding a user's selection of call restrictions using the display of the mobile terminal, nowhere does the cited portion of Kaplan disclose or suggest "providing a listing of numbers from a phone book of the mobile terminal to a display of the mobile terminal" and/or "receiving a designation of ones of the displayed listing of numbers", as recited by Claim 12. Nor does the Office Action rely on Mitchell, Morriss, and/or Bkanich to provide these recitations. Thus, Applicants submit that Claim 12 is separately patentable over the cited references for at least these reasons. Also, Claim 29 recites system recitations corresponding to the method of Claim 12, and as such, is separately patentable for at least similar reasons.

Also, Claim 20 recites, in part, that "the usage time limitation includes a limitation on times of day when the mobile terminal may be used". The Office Action asserts that Morriss discloses this recitation in one or more of Paragraphs 0011, 0051, 0053 and/or 0055. *See* Office Action, Page 10.

Applicants respectfully disagree. Morriss is directed to "a method and apparatus for remotely activating a restrictive operating mode of a wireless communication device in the event that the wireless device is lost or stolen. Morriss, Page 1, Paragraph 0011. More particularly, Morriss describes transmitting a wireless data message to a lost or stolen wireless device/mobile terminal including a restrictive mode activation/deactivation password to activate and/or deactivate a restrictive operating mode, where the mobile terminal is only capable of communicating with restricted target devices, such as other devices and/or services associated with the owner of the mobile terminal. *See* Morriss, Paragraphs 0035, 0036, 0042, 0043, 0051 and 0053. As further provided in Paragraph 0055 of Morriss:



In re: Hill et al.  
Serial No.: 10/736,079  
Filed: December 15, 2003  
Page 16

In the event that the received message or input includes the RMA password, the wireless device automatically places (411) itself in a restrictive operating mode in which it may only initiate a communication with one or more restricted target devices. That is, once the wireless device is placed in the restrictive operating mode in accordance with the present invention, the wireless device's operational software will only permit the device to place calls or send messages to the restricted target device(s). Notwithstanding the foregoing, the wireless device may still be used for other purposes, such as to supply the time of day, to play games or run other local applications that may be stored on the device, and to listen to music or ring tones stored on the device, just to name a few. Alternatively, the wireless device may be programmed to prohibit all use of the wireless device except for contacting the restricted target device(s) once the device is placed in the restrictive operating mode. The identities and contact information of the restricted target device(s) are preferably stored in the wireless device by the device's owner or wireless service provider prior to receipt of the message containing the RMA password, but may optionally be included in such message.

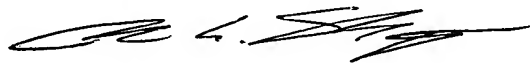
Morriss, Page 7, Paragraph 0055 (*emphasis added*). In other words, Morriss describes that, in the restrictive operating mode, the wireless device may still be used to supply the time of day. However, nowhere do the cited portions of Morriss appear to describe "a limitation on times of day when the mobile terminal may be used", as recited by Claim 20. Nor does the Office Action rely on Mitchell, Morriss, and/or Bekanich to provide these recitations. Thus, Applicants submit that Claim 20 is separately patentable over the cited references for at least these reasons.

In re: Hill et al.  
Serial No.: 10/736,079  
Filed: December 15, 2003  
Page 17

**Conclusion**

In view of the above, Applicants submit that the pending claims are in condition for allowance and respectfully request allowance of the present application. If further informalities are noted, the Examiner is encouraged to contact the undersigned by telephone to expedite allowance of the present application.

Respectfully submitted,



Rohan G. Sabapathypillai  
Registration No. 51,074

Myers Bigel Sibley & Sajovec, P.A.  
Post Office Box 37428  
Raleigh, NC 27627  
Telephone (919) 854-1400  
Facsimile (919) 854-1401

**CERTIFICATE OF MAILING**

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to Mail Stop Amendment, Commissioner for Patents, PO Box 1450, Alexandria, VA, 22313-1450, on April 21, 2006.



Betty-Lou Rosser